REMARKS

Favorable reconsideration of this application, in light of the preceding amendments and following remarks, is respectfully requested.

Claims 17-35 are pending in this application. Claim 17 is the sole independent claim and is currently amended.

Applicants note with appreciation the Examiner's indication that the references cited in the Information Disclosure Statement filed August 22, 2008 have been considered.

DISCUSSION OF EXAMPLE EMBODIMENTS

A non-limiting example embodiment is described to assist the Examiner in understanding the function of the present application and the differences between the present application and Hardy. Applicants submit that this description is only to assist the Examiner's understanding and should not limit any of claims 17-35 in any way. Instead, each claim should be interpreted solely based upon the limitations presented therein.

According to a non-limiting example embodiment, the security module 10 and the receiver 11 are jointly denominated the devices. The security module 10 may be, for example, in the form of a microchip card or a module including a chip. The security module 10 may contain a private asymmetric key PAKV of a pair of asymmetric keys. This key may be introduced into the security module 10, for example, at the time the module is manufactured or at a later stage, in a managing data centre or by a secure connection between said managing centre and the security module. The private asymmetric key PAKV may be stored in a non-volatile memory of the module.

According to a non-limiting example embodiment, the receiver 11 may be a box connected to a television set. It may contain a public asymmetric key PAKB

from the pair of asymmetric keys. This public key may be matched to the private key of the security module. The public key PAKB may also be programmed during the manufacture of the receiver.

ENTRY OF AMENDMENT AFTER FINAL REJECTION

Entry of the Amendment is requested under 37 C.F.R. § 1.116 because the Amendment: a) places the application in condition for allowance for the reasons discussed herein; b) does not present any additional claims without canceling the corresponding number of final rejected claims; and/or c) places the application in better form for an appeal, if an appeal is necessary. Entry of the Amendment is thus respectfully requested.

REJECTIONS UNDER 35 U.S.C. § 102

Claims 17-35 stand rejected under 35 U.S.C. § 102(e) as being anticipated by EP 0 537 971 B1 to Hardy et al. ("Hardy"). Applicants respectfully traverse this rejection for the reasons detailed below.

It is alleged in the Office Action that Hardy anticipates the limitations of independent claim 17 because teaches a method of data exchange as required by claim 17.

Hardy is directed to a method of secure communication between a variety of user equipments. In Hardy, communication between terminals 103 and 109 uses several key generation encryption algorithms. According to the Hardy method, the first step includes determining a key generator algorithm common to both terminals from a key management database within terminals 103 and 109. Once such an algorithm is found, a key is sent to these devices in order to enable them to encrypt/decrypt data that is exchanged between them. FIG. 3 illustrates a portion of a message sequence for automatically *initiating* secure communication

between terminals 103 and 109. As illustrated in FIG. 3, the public key management mode involves exchange of four messages, including an Access Domain and Capabilities (AD&C) Message 211. Access Domain and Capabilities (AD&C) Message 211 provides, among other things, a choice of key generator (KG) algorithm selected. FIG. 4 illustrates method 200, comprising the steps of exchanging Access Domain and Capabilities (AD&C) Messages in block 211. Namely, the Hardy method of data exchange includes initialization of the encryption keys as the first step. Additionally, the keys in the Hardy method are symmetric.

As such, Hardy fails to anticipate at least the steps of "encrypting said first random number by said first encrypting key, **the first encrypting key previously initialised in the first device**, [and] encrypting said second random number by said second encrypting key, **the second encrypting key previously initialised in the second device**," as required by independent claim 17.

Hardy fails to anticipate each and every limitation of claim 17. Claims 18-35, dependent on independent claim 17, are patentable for the reasons stated above with respect to claim 17 as well as for their own merits.

Applicants, therefore, respectfully request that the rejection to claims 17-35 under 35 U.S.C. § 102(b) be withdrawn.

CONCLUSION

In view of the above remarks and amendments, the Applicants respectfully submit that each of the pending objections and rejections has been addressed and overcome, placing the present application in condition for allowance. A notice to that effect is respectfully requested. If the Examiner believes that personal communication will expedite prosecution of this application, the Examiner is invited to contact the undersigned.

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact Donald J. Daley at the telephone number of the undersigned below.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 08-0750 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; particularly, extension of time fees.

Respectfully submitted,

HARNESS, DICKEY, & PIERCE, P.L.C.

By _____

Donald J. Daley, Reg. No. 34,313
P.O. Box 8910
Reston, Virginia 20195
(703) 668-8000

DJD/AZP:akp
AZP